(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. April 2007 (26.04.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/045395 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2006/009861

(22) Internationales Anmeldedatum:
11. Oktober 2006 (11.10.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
05022902.0 20. Oktober 2005 (20.10.2005) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **UBS AG** [CH/CH]; Bahnhofstrasse 45, CH-8001 Zürich (CH).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HILTGEN, Alain P.** [CH/CH]; Viktoriastrasse 23, CH-8057 Zürich (CH).

(74) Anwalt: **SCHMIDT, Steffen, J.**; WUESTHOFF & WUESTHOFF, Schweigerstrasse 2, 81541 München (DE).

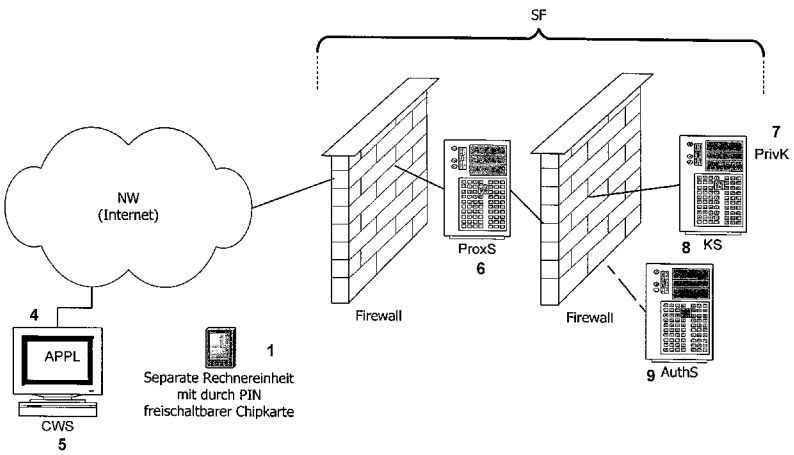
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

WO 2007/045395 A1

(54) Title: DEVICE AND METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS IN A SERVER-CLIENT COMPUTER NETWORK SYSTEM

(54) Bezeichnung: VORRICHTUNGEN UND VERFAHREN ZUM DURCHFÜHREN VON KRYPTOGRAPHISCHEN OPERATIONEN IN EINEM SERVER-CLIENT-RECHNERNETZWERKSYSTEM



1 ... INDIVIDUAL COMPUTER UNIT PROVIDED WITH A FREELY SWITCHABLE CHIP CARTE BY MEANS OF A PIN
4 ... APPLICATION
5 ... CLIENT COMPUTER WORKSTATION
6 ... PROXY SERVER
7 ... PRIVATE KEY
8 ... CRYPTOGRAPHY SERVER COMPUTER SYSTEM
9 ... AUTHENTICATION SERVER

(57) Abstract: In a server-client computer network system for carrying out cryptographic operations between a client computer workstation and a cryptography server computer system, a computer software programs for communication therebetween are installed in the client computer workstation and in the cryptography server computer system. Said computer software programs are executed in such a way that, when the client computer workstation transmits a request for carrying out a cryptographic operation to the cryptography server computer system, said computer workstation receives an answer therefrom. For this purpose, the cryptography server computer system requests a strong authentication from the client computer workstation. In response, the client computer workstation engages the key of the user thereof for producing said strong authentication. In the case of the successful authentication, the client computer workstation receives a release for initiating one or several cryptographic operations with the aid of the private key. According to said invention, the privet key is stored in the cryptography server computer system and cryptographic operation(s) is (are) authorised for a fixed short time after the successful authentication for carrying out the cryptographic operation(s) requested by the computer software program operating on the client computer workstation. At the same time, the client computer workstation puts at the disposal of the application software program the result of the cryptographic operation(s).

[Fortsetzung auf der nächsten Seite]

(84) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: In einem Server-Client-Rechnernetzwerksystem sind zum Durchführen von kryptografischen Operationen über ein Netzwerk zwischen einer Client-Rechner-Arbeitsstation und einem Kryptografie-Server-Rechnersystem, in der Client-Rechner-Arbeitsstation und in dem Kryptografie-Server-Rechnersystem zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert. Diese Computersoftware-Programme werden ausgeführt, damit, wenn die Client-Rechner-Arbeitsstation eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem richtet, diese von dem Kryptografie-Server-Rechnersystem beantwortet wird. Dazu fordert das Kryptografie-Server-Rechnersystem von der anfragenden Client-Rechner-Arbeitsstation eine starke Authentifizierung an. Als Reaktion hierauf greift die Client-Rechner-Arbeitsstation unter einer starken Authentifizierung auf einen Schlüssel ihres Nutzers zu. Bei erfolgreicher Authentifizierung erhält die Client-Rechner-Arbeitsstation eine Freigabe dafür, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel zu initiieren. Dabei ist erfindungsgemäß der private Schlüssel auf dem Kryptografie-Server-Rechnersystem abgelegt, und die kryptografische/n Operation/en wird/werden nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen, um die von einer auf der Client-Rechner-Arbeitsstation ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en auszuführen. Dabei stellt die Client-Rechner-Arbeitsstation das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung.

VORRICHTUNGEN UND VERFAHREN ZUM DURCHFÜHREN VON KRYPTOGRAPHISCHEN OPERATIONEN IN EINEM SERVER-CLIENT-RECHNERNETZWERKSYSTEM

Beschreibung

Hintergrund der Erfindung

Die vorliegende Erfindung betrifft ein Server-Client-Rechnernetzwerksystem zum Durchführen von kryptografischen Operationen und ein Verfahren zum Durchführen von kryptografischen Operationen in einem solchen Rechnernetzwerksystem. Insbesondere betrifft die Erfindung solche Rechnernetzwerksysteme, bei denen ein Nutzer (aus einer Vielzahl von Nutzern) mittels einer Netzwerk-Arbeitsstation eine sichere Verbindung mit einem zentralen Rechnersystem initiieren und anschließend über diese Verbindung Datenkommunikation mit dem zentralen Rechnersystem abwickeln möchte.

Ein solches Szenario wird zum Beispiel im Rahmen von sog. online banking realisiert. Dabei verfügt ein Kunde eines Bankinstitutes über eine Netzwerk-Arbeitsstation (Rechnereinheit, zum Beispiel PC, mit alphanumerischer Anzeige, Tastatur und Schnittstelle zum Netzwerk, zum Beispiel Internet), auf der ein sog. Browser installiert ist. WWW-Browser sind Computerprogramme zum Betrachten von Webseiten im Internet (= WWW-Seiten). Mit dieser Netzwerk-Arbeitsstation kann sich der Kunde sich über das Netzwerk mit dem zentralen Rechnersystem des Bankinstitutes verbinden und Banktransaktionen (zum Beispiel Kontoabfragen, Überweisungen, Depotbewegungen, oder dergl.) ausführen. Ein anderes, ebenfalls von der Erfindung erfasstes Szenario ist das Versenden von e-mails von einem Kunden/Partner einer Institution, (zum Beispiel des Bankinstitutes) zu der Institution im Rahmen von vertraulichem Schriftwechsel, der zu diesem Zweck verschlüsselt wird. Aber auch Internet-Auktionen, virtuelle Kaufhäuser, oder dergl. basieren auf einem derartigen Szenario.

Dabei sind derartige Netzwerkverbindungen zum Schutz gegen nicht erwünschte Eindringlinge oder Kriminelle durch die unterschiedlichsten Mechanismen geschützt. Dazu zählen sog. PIN/TAN – Verfahren, bei denen ein Nutzer sich gegenüber einer Institution mittels einer Zugangsnummer und einer nur ihm bekannten statischen Kennung (personal identification number = PIN) zu erkennen gibt. Anschließend kann er bei der Institution bestimmte Transaktionen ausführen, zu deren Abschluss

er eine einmal gültige Transaktionsnummer (= TAN) einzugeben hat. Derartige Verfahren sind zwar weit verbreitet, aber relativ unsicher, da die PIN statisch ist und solange gültig ist, bis der Nutzer sie gegen eine andere austauscht. Die lediglich einmal gültige TAN wird aus einer sog. Streichliste genommen, welche dem Nutzer elektronisch oder als Kopie zugestellt worden ist.

Abgesehen von dem Entwenden der schriftlich niedergelegten oder als Datei vorgehaltenen PIN/TAN Information ist es auch möglich, durch einen sog. Mittelsmann-Angriff (man-in-the-middle attack) in der Netzwerkverbindung zwischen dem Nutzer und der Institution diese Daten in unerlaubter Weise zu erlangen und für kriminelle Zwecke zu nutzen (ohne dass der rechtmäßige Nutzer dies bemerkt). Ein Man-In-The-Middle-Angriff ist eine Angriffsform, bei der Angreifer entweder physikalisch, aber heute meist logisch, zwischen den beiden Kommunikations-partnern steht und mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern hat. Er kann die Informationen nach Belieben einsehen und sogar manipulieren. Diese Situation kann zum Beispiel dadurch erreicht werden, dass der Angreifer Kontrolle über einen Router hat, durch den der Datenverkehr geschleust wird. Es ist auch möglich, dass der Angreifer eine falsche Zieladresse für die Internet-Kommunikation vorgibt und leitet dadurch den Verkehr durch seinen eigenen Rechner (Poison Routing). Am effektivsten lässt sich dieser Angriffsform mit einer Verschlüsselung der Datenpakete entgegenwirken, wobei allerdings die Zertifikate der Schlüssel über ein zuverlässiges Medium verifiziert werden sollten. Es muss also eine gegenseitige Authentifizierung stattfinden. Dazu müssen die beiden Kommunikationspartner auf anderem Wege ihre digitalen Zertifikate oder einen gemeinsamen Schlüssel ausgetauscht haben, d.h. sie müssen sich "kennen". Sonst kann z.B. ein Angreifer bei einer ersten Verbindungsaufnahme beiden Kommunikationspartner falsche Schlüssel vortäuschen und somit auch den verschlüsselten Datenverkehr mitlesen.

Um dies zu erschweren, wurden Protokolle wie zum Beispiel das von der Firma Netscape entwickelte SSL (Secure Sockets Layer) Übertragungsprotokoll vereinbart, die es erlauben, verschlüsselte Verbindungen über eine potenziell unsichere Internet-Verbindung aufzubauen. Es wird heute von allen gängigen WWW-Browsern unterstützt und kommt in der Praxis (z.B. beim online-Banking) zum Einsatz. Der URL (Unique Resource Locator) einer WWW-Seite, die gemäß dem SSL Protokoll verschlüsselt übertragen wird, ist erkennbar am Präfix https:// (statt http:// beim unverschlüsselten Datentransfer). Außerdem zeigen die meisten WWW-Browser die

unter dem SSL Protokoll zustande gekommene Verbindung durch ein Symbol (z.B. ein Vorhängeschloss) in der Statusleiste an.

Das SSL-Protokoll besteht aus zwei Schichten (layers): Zu Grunde liegt in der untersten Ebene das SSL Record Protocol, das zur Kapselung verschiedener höherer Protokolle (higher level protocols) dient. Ein Beispiel dafür ist das SSL Handshake Protocol zur Authentifizierung von Client und Server und der Vereinbarung des verwendeten Verschlüsselungsverfahrens, oder das HTTP Protokoll zur Übertragung von Webseiten.

Es gibt verschiedene SSL-Varianten, die zum Teil auch mit TLS (Transport Layer Security) bezeichnet werden. Die jeweils verwendete SSL-Variante wird beim Verbindungsaufbau zwischen dem WWW-Browser und dem WWW-Server automatisch ausgehandelt. Zur Verschlüsselung der Daten bei einer SSL-Verbindung kommt meist das Verschlüsselungs-Verfahren RC4 zum Einsatz. Die kryptografische Sicherheit dieses Algorithmus ist abhängig von der Länge des Schlüssels, der zur Verschlüsselung eingesetzt wird.

Beim Aufbau einer SSL-Verbindung generiert der WWW-Browser einen zufälligen Schlüssel (Sitzungsschlüssel = Session Key), der für die Dauer der Verbindung zur Verschlüsselung genutzt wird. Damit die SSL-Verbindung nicht abgehört werden kann, muss zunächst dieser Sitzungsschlüssel auf einem sicheren Weg zum WWW-Server übertragen werden. Um dies zu gewährleisten, wird der Sitzungsschlüssel seinerseits mit einem öffentlichen Schlüssel-Verfahren (Public Key Verfahren), zum Beispiel RSA, verschlüsselt. Dazu präsentiert der WWW-Server seinen öffentlichen RSA-Schlüssel; der WWW-Browser verschlüsselt damit den Sitzungsschlüssel und übermittelt das Ergebnis wieder dem WWW-Server. Erst danach wird die eigentliche Datenkommunikation aufgenommen.

Wesentlich für die Sicherheit des beschriebenen Verfahrens ist dabei die Authentizität des öffentlichen Schlüssels des WWW-Servers. Ein potenzieller Angreifer könnte in einem Täuschungsversuch einen fiktiven öffentlichen RSA-Schlüssel darbieten und auch im weiteren die Rolle des "echten", vom Nutzer eigentlich angesprochenen WWW-Servers übernehmen. Die Kommunikation würde dann zwar verschlüsselt stattfinden, der Angreifer könnte aber trotzdem mit Hilfe des ihm bekannten Sitzungsschlüssel den Klartext ermitteln. Um derartige Täuschungsversuche zu erschweren, trägt der öffentliche Schlüssel des WWW-Servers zusätzliche

Informationen, die seine Identität (Name des Servers, Organisation, die den Server betreibt, ...) beschreiben. Die Integrität dieser Informationen ist durch eine digitale Signatur geschützt; alles zusammen wird als Zertifikat nach dem X.509 Standard bezeichnet. Dieses Zertifikat wird von einer Zertifizierungsstelle (Certificate Authority = CA) nach der Prüfung der Identität des Server-Betreibers ausgestellt.

Ein WWW-Browser kann also den öffentlichen Schlüssel eines ihm unbekannten WWW-Servers als authentisch erkennen, wenn er die digitale Signatur der Zertifizierungsstelle überprüfen kann. Dazu benötigt er den öffentlichen Schlüssel der Zertifizierungsstelle. Die öffentlichen Schlüssel einiger Zertifizierungsstellen sind den Standard-Browsern bereits bekannt; Zertifikate von WWW-Servern, die von diesen Zertifizierungsstellen signiert sind, werden daher unmittelbar akzeptiert. Es gibt jedoch auch die Möglichkeit, dem Browser die öffentlichen Schlüssel weiterer Zertifizierungsstellen bekannt zu machen, so dass auch deren Zertifikate überprüft werden können.

Der öffentliche Schlüssel einer Zertifizierungsstelle ist (wie auch der öffentliche Schlüssel eines WWW-Servers) ein X.509-Zertifikat, das seinerseits von einer übergeordneten Zertifizierungsstelle signiert sein kann. Somit kann der Browser auch die Echtheit des Zertifizierungsstellen-Schlüssels überprüfen, wenn er die übergeordnete Zertifizierungsstelle kennt. Die Entscheidung über die Vertrauenswürdigkeit einer Zertifizierungsstelle, die nicht durch die digitale Signatur einer anderen Instanz gedeckt ist, kann aber nur der Benutzer selbst entscheiden. Wenn der WWW-Browser von einem WWW-Server ein Zertifikat erhält, dessen Echtheit er nicht nachprüfen kann, wird der Benutzer zu einer Entscheidung über das weitere Vorgehen aufgefordert.

Die Schritte zum Aufbau einer herkömmlichen SSL Verbindung zwischen Client und (Proxy) Server laufen wie folgt ab:

1. Der Client sendet eine Verbindungsanfrage an den Server.

2. Der Server antwortet mit derselben Nachricht und sendet eventuell ein Zertifikat.
3. Der Client versucht, das Zertifikat zu authentifizieren (bei Misserfolg wird die Verbindung abgebrochen). Dieses Zertifikat enthält den öffentlichen Schlüssel des Servers.
4. Nach erfolgter Authentifizierung erstellt der Client das "pre-master secret", verschlüsselt dieses mit dem öffentlichen Schlüssels des Servers und sendet es an den Server. Daraus erzeugt der Client ebenfalls das "master secret".
5. Der Server entschlüsselt das "pre-master-secret" mit seinem privaten Schlüssel und erstellt das "master secret".
6. Client und Server erstellen aus dem "master secret" den "session-key". Das ist ein einmalig benutzter symmetrischer Schlüssel, der während der Verbindung zum Ver- und Entschlüsseln der Daten genutzt wird. SSL unterstützt für die symmetrische Verschlüsselung mit diesem "session-key" u.a. die Verschlüsselungsverfahren DES und Triple DES.
7. Client und Server tauschen mit diesem "session-key" verschlüsselte Nachrichten aus und signalisieren damit ihre Kommunikationsbereitschaft.
8. Die SSL-Verbindung ist aufgebaut.

Ein Proxy Server ist ein Computerprogramm, das auf einer separaten Rechnereinheit, aber auch auf der gleichen Rechnereinheit wie das eigentliche Web Serverprogramm ablaufen kann und im Datenverkehr zwischen der über das Netzwerk anfragenden Arbeitsstation und dem Web Serverprogramm vermittelt. Aus Sicht des Web Servers verhält sich der Proxy Server wie ein Client, dem Client gegenüber wie ein Web Server. Im einfachsten Fall leitet der Proxy Server die Daten einfach weiter. Ein sog. http-Proxy Server, der zwischen Webbrowser (Client) und Web Server vermittelt, hat insbesondere bei sicherheitskritischen Anwendungen, wie online banking, eine Filterfunktion, so dass bestimmte Kategorien von Web seiten oder einzelne Webseiten für den Benutzer gesperrt und/oder Zugriffe darauf protokolliert werden. Auch kann der Inhalt auf schädliche Programme oder Funktionen durchsucht werden. Außerdem dient ein Proxy Server der Zugriffssteuerung: Damit der Web Server nicht frei über das Internet erreichbar ist, steuert und kontrolliert ein davor geschalteter Proxy Server den Zugriff darauf. Ein Angreifer kann dann den Web Server nicht mehr direkt angreifen, sondern nur den Proxy Server. Es kann auch der Zugriff von Clients auf Web Server nur über einen Proxy Server ermöglicht werden. Dabei kann der Proxy Server auch als Reverse Proxy konfiguriert sein. Dazu ist er logisch vor den anderen Web Servern und Applikations- Servern aufgestellt. Verbindungsanfragen aus dem Internet an einen

Web Server werden durch den Proxy Server bearbeitet, welcher die Anfrage entweder vollständig selbst beantwortet, oder sie teilweise oder ganz an den bzw. einen der nachgeordneten Web Server weiterleitet. Der Reverse Proxy Server stellt ein weiteres Glied in der Sicherheitskette dar und trägt so zur Sicherheit der Web Server bei. Um sichere Webseiten schnell zu erzeugen, wird die SSL Verschlüsselung nicht vom Webserver selbst erledigt, sondern durch einen Reverse Proxy Server, der mit einer entsprechenden Beschleunigungshardware ausgestattet ist.

Die US 2001/0014158 beschreibt ein Client-Server-System, bei dem ein privater Schlüssel auf einem Verschlüsselungsserver gespeichert wird. Um den Schlüssel nutzen zu können, greift der Benutzer über sein Client-System auf den Server zu. Um den Schlüssel zu verwenden, d.h. für den Zugriff auf den Schlüssel, ist es erforderlich, das der Benutzer ein Passwort eingibt, welches dem Verschlüsselungsserver übermittelt wird. Daraufhin übermittelt der Verschlüsselungsserver den privaten Schlüssel des Benutzers in verschlüsselter Form an das Client-System.

Die WO 01/48948 beschreibt ein System, bei dem ein Schlüssel in einem Server bzw. einer Netzwerkeinrichtung erzeugt wird. Der Schlüssel wird sodann an einen Client bzw. ein Terminal übermittelt. Um die Sicherheit bei Verwendung des Schlüssels zu erhöhen, wird der Schlüssel in periodischen oder zufälligen Abständen gewechselt.

Zusammenfassend ist festzustellen, dass die heute verfügbaren Mechanismen zur vertraulichen Datenkommunikation zwischen einem Nutzer aus einer Vielzahl von Nutzern (zum Beispiel Bankkunden) und einer Institution (zum Beispiel einem Bankinstitut) aus den unterschiedlichsten Gründen nicht sicher sind. Dazu zählt, dass ein Nutzer in der Regel nicht über die notwendigen technischen Fachkenntnisse verfügt, und dass die Bedienung der Hard- und Software im Fall komplexerer Sicherheitsmechanismen für viele der Nutzer zu kompliziert ist und daher von ihnen abgelehnt wird. Außerdem ist vielfach das Bewusstsein zu wenig ausgeprägt, dass nur bei möglichst hoher Disziplin im Umgang mit sicherheitsrelevanter Information deren Missbrauch und damit ein Schaden für den einzelnen Nutzer / die Institution zu vermeiden oder für den Kriminellen zumindest zu erschweren ist.

Der Erfindung zugrunde liegendes technisches Problem

Die Erfindung hat die Aufgabe, ein sicheres Rechnernetzwerk und ein Verfahren zum Aufbau einer sicheren Rechnernetzwerkverbindung bereitzustellen, damit ein Nutzer (aus einer Vielzahl von Nutzern) in dem Netzwerk mittels einer Netzwerk-Arbeitsstation auf seine Schlüssel mit hoher Sicherheit gegenüber unerwünschten Zugriffen Dritter zugreifen kann.

Erfindungsgemäße Lösung

Zur Lösung dieser Aufgabe stellt die Erfindung ein Rechnernetzwerksystem mit den Merkmalen des Anspruchs 1 bereit.

Technische Merkmale der Erfindung

Dazu sind in einem Server-Client-Rechnernetzwerksystem zum Durchführen von kryptografischen Operationen über ein Netzwerk zwischen einer Client-Rechner-Arbeitsstation und einem Kryptografie-Server-Rechnersystem, in der Client-Rechner-Arbeitsstation und in dem Kryptografie-Server-Rechnersystem zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert. Diese Computersoftware-Programme werden ausgeführt, damit, wenn die Client-Rechner-Arbeitsstation eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem richtet, diese von dem Kryptografie-Server-Rechnersystem beantwortet wird. Dazu fordert das Kryptografie-Server-Rechnersystem von der anfragenden Client-Rechner-Arbeitsstation eine starke Authentifizierung an. Als Reaktion hierauf greift die Client-Rechner-Arbeitsstation bei erfolgreicher Authentifizierung auf einen Schlüssel ihres Nutzers zu. Bei erfolgreicher Authentifizierung erhält die Client-Rechner-Arbeitsstation eine Freigabe dafür, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel zu initiieren. Dabei ist erfindungsgemäß der private Schlüssel auf dem Kryptografie-Server-Rechnersystem abgelegt. Der private Schlüssel wird nicht über das Netzwerk (NW) übertragen, sondern verbleibt stets in dem Kryptografie-Server-Rechnersystem. Die kryptografische/n Operation/en wird/werden nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen, um die von einer auf der Client-Rechner-Arbeitsstation ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en auszuführen. Dabei stellt die Client-Rechner-Arbeitsstation das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung.

Durch die Erfindung bewirkte technische Effekte

Die sog. Man-In-The-Middle-Angriffe sind ausgeschlossen, da aufgrund der erfindungsgemäßen Konfiguration die Client-Rechner-Arbeitsstation darüber informiert ist, mit welchem Kryptografie-Server-Rechnersystem die Verbindung besteht (Server Authentification), und der Schlüssel durch die starke Authentifizierung geschützt ist, weil er nicht über das Netzwerk übertragen wird, sondern stets in dem Kryptografie-Server-Rechnersystem verbleibt; dennoch steht der private Schlüssel dem Nutzer zur Verfügung.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung

Die kryptografischen Operationen können das Signieren eines Hashwertes oder das Entschlüsseln (Dechiffrieren) eines geheimen Schlüssels umfassen.

Bei dem erfindungsgemäßen Server-Client-Rechnernetzwerksystem kann das Kryptografie-Server-Rechnersystem zusätzlich einen Proxy Server und/oder einen Authentifizierungs-Server haben.

Für eine starke Authentifizierung kann ein für kurze Zeit gültiges, und/oder einmaliges, und/oder dynamisch erzeugtes Legitimationsmittel zwischen der Client-Rechner-Arbeitsstation und dem Kryptografie-Server-Rechnersystem ausgetauscht werden. Insbesondere kann das Legitimationsmittel ein Passwort, ein Kennsatz, oder dergl. sein. Es sind jedoch auch andere starke Authentifizierungen im Rahmen der vorliegenden Erfindung möglich und einsetzbar.

Bei dem erfindungsgemäßen Server-Client-Rechnernetzwerksystem ist die starke Authentifizierung in einem in einem Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation implementiert, wobei das Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation einen Nutzer vorzugsweise im Dialog auffordert, dessen ihn gegenüber dem Kryptografie-Server-Rechnersystem identifizierende Kennung einzugeben, und nach Eingabe der Kennung des Nutzers die starke Authentifizierung anstößt.

Weiterhin wird in dem erfindungsgemäßen Server-Client-Rechnernetzwerksystem in dem Kryptografie-Server-Rechnersystem die starke Authentifizierung überprüft, und bei korrekter Authentifizierung an die Client-Rechner-Arbeitsstation eine erfolgreiche Authentifizierung signalisiert.

Erfindungsgemäß fordert die Client-Rechner-Arbeitsstation einen Nutzer dazu auf, dessen Vertragsnummer oder eine sonstige Kennung einzugeben, mit der die Institution, zu deren Server-Rechnersystem er Zugang haben möchte, ihn identifizieren kann. Nach Eingabe der Vertragsnummer gibt bei dem erfindungsgemäßen Server-Client-Rechnernetzwerksystem die Client-Rechner-Arbeitsstation für den Nutzer nach Eingabe dessen Kennung eine Zeichenkette für den Nutzer (zum Beispiel auf einem Bildschirm oder dergl.) aus. Diese Zeichenkette hat der Nutzer (vorzugsweise innerhalb einer vorbestimmten Zeit von wenigen Minuten) in eine separate Rechnereinheit einzugeben. Vorher wurde die separate Rechnereinheit mit einer gesicherten Chipkarte verbunden und mittels einer dem Nutzer bekannten PIN (zum Beispiel durch Eingabe von dem Nutzer über eine Tastatur der Rechnereinheit) ist die gesicherte Chipkarte frei geschaltet worden. Daraufhin verknüpft die separate Rechnereinheit mit der Chipkarte unter Anwendung einer Verknüpfungsvorschrift die Zeichenkette mit einem in der Chipkarte abgelegten Schlüssel und gibt dem Nutzer eine Antwortzeichenkette aus. Diese Antwortzeichenkette gibt der Nutzer (zum Beispiel über eine Tastatur) in die Client-Rechner-Arbeitsstation ein. Die Client-Rechner-Arbeitsstation sendet diese Antwortzeichenkette an das Kryptografie-Server-Rechnersystem.

Es handelt sich hierbei also um ein interaktives Authentfizierungssystem, das Chipkarten-basiert ist. Ein Vorteil dieses Verfahrens ist die Kurzzeitigkeit der Geltung der Schlüssel/Daten. Zudem wird durch die erfindungsgemäße Vorgehensweise sichergestellt, dass die Generierung des Codes erst beim Verbindungsaufbau erfolgt. Dieser Code wird jedes Mal neu berechnet und ist nur für eine kurze Zeit gültig. Auf der Chipkarte ist ein Schlüssel gespeichert, der eindeutig einer (Vertrags-)Beziehung zwischen dem Nutzer und dem Betreiber des Kryptografie-Server-Rechnersystems zugeordnet ist. Der Inhalt der Chipkarte ist geschützt und kann weder kopiert noch von Dritten offen gelegt werden. Denn es werden nie alle Sicherheitselemente gleichzeitig über das Internet übertragen.

Erfindungsgemäß wird in dem Server-Rechnersystem (genauer gesagt, vorzugsweise in dem Kryptografie-Server-Rechnersystem) unter Anwendung einer entsprechenden Verknüpfungsvorschrift die dem Nutzer ausgegebene Zeichenkette mit dem in dem Server-Rechnersystem abgelegten privaten (vorzugsweise symmetrischen) Schlüssel verknüpft. Das Ergebnis der Verknüpfung wird mit der von dem Nutzer in die Client-Rechner-Arbeitsstation eingegebenen Antwortzeichenkette verglichen. Bei

Übereinstimmung wird an die Client-Rechner-Arbeitsstation eine erfolgreiche Authentifizierung signalisiert.

Bei nicht erfolgreicher Authentifizierung bricht das Computer-Softwareprogramm die Kommunikation ab oder baut die gewünschte Verbindung gar nicht erst auf.

Des Weiteren betrifft die Erfindung ein Verfahren zum Durchführen von kryptografischen Operationen in einem Server-Client-Rechnernetzwerksystem über ein Netzwerk zwischen einer Client-Rechner-Arbeitsstation und einem Kryptografie-Server-Rechnersystem mit den vorstehend erläuterten Eigenschaften und Merkmalen. Außerdem betrifft die Erfindung ein Server-Rechnersystem, sowie eine Client-Rechner-Arbeitsstation, konfiguriert und programmiert zur Ausführung dieses Verfahrens.

Schließlich ist Gegenstand der Erfindung auch ein Computerprogrammprodukt mit computerausführbaren Programm-Objektcode zur Realisierung des Verfahrens, wobei der Programm-Objektcode, wenn er in einem oder mehreren Computern ausgeführt wird, dazu eingerichtet ist, in einem Server-Client-Rechnernetzwerksystem eine sichere Rechnernetzwerkverbindung nach einem der vorhergehenden Ansprüche zu bewirken.

Kurzbeschreibung der Zeichnung

Weitere Eigenschaften, Vorteile, mögliche Abwandlungen und Alternativen sind in der nachstehenden Beschreibung von Ausführungsbeispielen der Erfindung unter Bezugnahme auf die Fig. veranschaulicht. Dabei ist:

in Fig. 1 eine Konfiguration eines erfindungsgemäßen Server-Client-Rechnernetzwerksystem schematisch veranschaulicht;

in Fig. 2 ein Ablauf der Schritte, die das erfindungsgemäße Server-Client-Rechnernetzwerksystem ausführt, schematisch veranschaulicht;

in Fig. 2a sind die Kategorien möglicher kryptografischen Operationen tabellarisch veranschaulicht; und

in Fig. 3 ein Ablauf der Schritte, die erfindungsgemäß zur starken Authentifizierung auszuführen sind, schematisch veranschaulicht.

Detaillierte Beschreibung erfindungsgemäßer Ausführungsbeispiele

Fig. 1 zeigt ein Server-Client-Rechnernetzwerksystem zum Durchführen von kryptografischen Operationen über ein Netzwerk NW, zum Beispiel das Internet. Dabei findet Kommunikation zwischen einer Client-Rechner-Arbeitsstation CWS, zum Beispiel dem PC eines Bankkunden mit Internetzugang, und einer Serverfarm SF der Bank statt, die unter anderem einem Kryptografie-Server-Rechnersystem KS umfasst. Auf der Seite des Bankkunden ist außerdem eine separate Rechnereinheit mit einer Chipkarte vorhanden, die durch Eingabe einer PIN freischaltbar ist. Wie in Fig. 1 veranschaulicht ist, umfasst die Serverfarm SF neben dem Kryptografie-Server-Rechnersystem KS zusätzlich einen – vorgeschalteten - Proxy Server ProxS und einen Authentifizierungs-Server AuthS.

In der Client-Rechner-Arbeitsstation CWS und in dem Kryptografie-Server-Rechnersystem KS sind zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert. Diese Computersoftware-Programme werden ausgeführt, damit, wenn die Client-Rechner-Arbeitsstation CWS eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem KS richtet, diese von dem Kryptografie-Server-Rechnersystem KS beantwortet wird.

Der Ablauf dieser Programme sowie der Ablauf der Schritte, die zur starken Authentifizierung auszuführen sind, ist in den Fig. 2 und 3 veranschaulicht.

Zunächst fordert das Kryptografie-Server-Rechnersystem KS von der anfragenden Client-Rechner-Arbeitsstation CWS eine starke Authentifizierung an.

Daraufhin greift die Client-Rechner-Arbeitsstation CWS unter einer starken Authentifizierung auf einen Schlüssel ihres Nutzers zu. Die Details hierzu sind weiter unten Unterbezugnahme auf Fig. 3 beschrieben. Bei erfolgreicher Authentifizierung erhält die Client-Rechner-Arbeitsstation CWS eine Freigabe dafür, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel privK zu initiieren. Der private Schlüssel privK ist auf dem Kryptografie-Server-Rechnersystem KS abgelegt. Im Übrigen ist die kryptografische Operation nur innerhalb eines

festgelegten, kurzen Zeitraums von etwa 0,2 ... 5 min nach der erfolgreichen Authentifizierung zugelassen wird um von einer auf der Client-Rechner-Arbeitsstation CWS ablaufenden Applikationsprogramm-Software Appl angeforderte kryptografische Operation auszuführen. Dabei stellt die Client-Rechner-Arbeitsstation CWS das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung.

Wie in Fig. 2a veranschaulicht ist, können die kryptografischen Operationen das Signieren eines Hashwertes oder das Entschlüsseln eines Schlüssels umfassen, wobei der Schlüssel symmetrisch sein kann, und/oder ein privater Schlüssel sein.

Wie in Fig. 2b veranschaulicht ist, kann die starke Authentifizierung ein für kurze Zeit gültiges, und/oder ein einmalig gültiges, und/oder dynamisch erzeugtes Legitimationsmittel verwenden, das zum Beispiel ein Passwort, ein Kennsatz, ein Ergebnis eines Anforderungs-Antwort-Ablaufes (Challenge-Response-Verfahren) oder dergl. sein kann und zwischen der Client-Rechner-Arbeitsstation CWS und dem Kryptografie-Server-Rechnersystem KS ausgetauscht wird.

Fig. 3 veranschaulicht die Abläufe im Zusammenhang mit der starken Authentifizierung. Diese ist – zumindest teilweise - in einem Computer-Softwareprogramm implementiert, das in der Client-Rechner-Arbeitsstation CWS abläuft. Dieses Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation CWS fordert einen Nutzer im Dialog auf, dessen ihn gegenüber dem Kryptografie-Server-Rechnersystem KS identifizierende Kennung einzugeben. Nach Eingabe der Kennung des Nutzers stößt Computer-Softwareprogramm die starke Authentifizierung an.

Dazu wird in dem Kryptografie-Server-Rechnersystem KS das Legitimationsmittel der starken Authentifizierung überprüft, und bei korrekter Authentifizierung wird an die Client-Rechner-Arbeitsstation CWS eine erfolgreiche Authentifizierung signalisiert.

Die Client-Rechner-Arbeitsstation CWS gibt für den Nutzer nach Eingabe dessen Kennung eine Zeichenkette für den Nutzer aus, die der Nutzer in eine separate Rechnereinheit einzugeben hat. Vorher muss die separate Rechnereinheit mit einer gesicherten Chipkarte verbunden worden sein und mittels einer PIN frei geschaltet worden sein. Die separate Rechnereinheit mit der Chipkarte verknüpft unter Anwendung einer Verknüpfungsvorschrift die eingegebene Zeichenkette mit einem in

der Chipkarte abgelegten Schlüssel. Daraufhin gibt die separate Rechnereinheit an den Nutzer eine Antwortzeichenkette aus. Diese Antwortzeichenkette hat der Nutzer in die Client-Rechner-Arbeitsstation CWS einzugeben. Die Client-Rechner-Arbeitsstation CWS sendet die Antwortzeichenkette zur Authentisierung an das Kryptografie-Server-Rechnersystem KS.

In dem Server-Rechnersystem SF wird unter Anwendung einer entsprechenden Verknüpfungsvorschrift die dem Nutzer ausgegebene Zeichenkette mit dem in dem Server-Rechnersystem SF abgelegten geheimen Schlüssel verknüpft. Das Ergebnis dieser Verknüpfung wird mit der von dem Nutzer in die Client-Rechner-Arbeitsstation eingegebenen Antwortzeichenkette verglichen. Bei Übereinstimmung wird an die Client-Rechner-Arbeitsstation CWS eine erfolgreiche Authentifizierung signalisiert.

Patentansprüche

1. Server-Client-Rechnernetzwerksystem zum Durchführen von kryptografischen Operationen über ein Netzwerk (NW) zwischen einer Client-Rechner-Arbeitsstation (CWS) und einem Kryptografie-Server-Rechnersystem (KS), wobei
in der Client-Rechner-Arbeitsstation (CWS) und in dem Kryptografie-Server-Rechnersystem (KS) zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert sind und ausgeführt werden, damit, wenn die Client-Rechner-Arbeitsstation (CWS) eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem (KS) richtet, diese von dem Kryptografie-Server-Rechnersystem (KS) beantwortet wird,
dadurch gekennzeichnet, dass
die Anfrage beantwortet wird, indem das Kryptografie-Server-Rechnersystem (KS) von der anfragenden Client-Rechner-Arbeitsstation (CWS) eine starke Authentifizierung anfordert,
worauf die Client-Rechner-Arbeitsstation (CWS) bei erfolgreicher Authentifizierung auf einen privaten Schlüssel (privK) ihres Nutzers zugreift, und
die Client-Rechner-Arbeitsstation (CWS) bei erfolgreicher Authentifizierung eine Freigabe dafür erhält, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel (privK) zu initiieren, wobei
   - der private Schlüssel (privK) auf dem Kryptografie-Server-Rechnersystem (KS) abgelegt ist und nicht über das Netzwerk (NW) übertragen wird, sondern stets in dem Kryptografie-Server-Rechnersystem (KS) verbleibt, und
   - die kryptografische/n Operation/en nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen wird/werden, um

die von einer auf der Client-Rechner-Arbeitsstation (CWS) ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en auszuführen, wobei

1.1. die Client-Rechner-Arbeitsstation (CWS) das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung stellt.

2. Server-Client-Rechnernetzwerksystem zum Durchführen von kryptografischen Operationen nach Anspruch 1, bei dem die kryptografischen Operationen

2.1. das Signieren eines Hashwertes oder

2.2. das Entschlüsseln eines Schlüssels

umfassen, wobei

2.2.1. der Schlüssel symmetrisch oder asymmetrisch sein kann, und/oder

2.2.2. ein privater, oder ein geheimer Schlüssel sein kann.

3. Server-Client-Rechnernetzwerksystem nach Anspruch 1 oder 2, bei dem das Kryptografie-Server-Rechnersystem (KS) zusätzlich einen Proxy Server (ProxS) und einen Authentifizierungs-Server (AuthS) hat.

4. Server-Client-Rechnernetzwerksystem nach einem der Ansprüche 1 bis 3, bei dem

4.1. die starke Authentifizierung ein

4.1.1. für kurze Zeit gültiges, und/oder

4.1.2. einmaliges, und/oder

4.1.3. dynamisches

Legitimationsmittel verwendet, das zwischen der Client-Rechner-Arbeitsstation (CWS) und dem Kryptografie-Server-Rechnersystem (KS) ausgetauscht wird.

5. Server-Client-Rechnernetzwerksystem nach Anspruch 4, bei dem das Legitimationsmittel ein Passwort, ein Kennsatz, oder ein Ergebnis eines Anforderungs-Antwort-Ablaufes ist.

6. Server-Client-Rechnernetzwerksystem nach Anspruch 4 oder 5, bei dem die starke Authentifizierung in einem Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation (CWS) implementiert ist, wobei

6.1. das Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation (CWS) einen Nutzer vorzugsweise im Dialog auffordert, dessen ihn gegenüber dem Kryptografie-Server-Rechnersystem (KS) identifizierende Kennung einzugeben, und

6.2. nach Eingabe der Kennung des Nutzers die starke Authentifizierung anstößt.

7. Server-Client-Rechnernetzwerksystem nach Anspruch 6, bei dem in dem Kryptografie-Server-Rechnersystem (KS)

7.1. das Legitimationsmittel der starken Authentifizierung überprüft wird, und

7.2. bei korrekter Authentifizierung an die Client-Rechner-Arbeitsstation (CWS) eine erfolgreiche Authentifizierung signalisiert wird.

8. Server-Client-Rechnernetzwerksystem nach Anspruch 6, bei dem die Client-Rechner-Arbeitsstation (CWS) für den Nutzer nach Eingabe dessen Kennung eine

Zeichenkette für den Nutzer ausgibt, die der Nutzer in eine separate Rechnereinheit einzugeben hat, die vorher mit einer gesicherten Chipkarte verbunden worden ist und mittels einer PIN frei geschaltet worden ist, worauf die separate Rechnereinheit mit der Chipkarte unter Anwendung einer Verknüpfungsvorschrift die Zeichenkette mit einem in der Chipkarte abgelegten Schlüssel verknüpft und dem Nutzer eine Antwortzeichenkette ausgibt, welche der Nutzer in die Client-Rechner-Arbeitsstation (CWS) einzugeben hat, und welche die Client-Rechner-Arbeitsstation (CWS) zur Authentisierung an das Kryptografie-Server-Rechnersystem (KS) sendet.

9. Server-Client-Rechnernetzwerksystem nach Anspruch 8, bei dem in dem Server-Rechnersystem (SF) unter Anwendung einer entsprechenden Verknüpfungsvorschrift die dem Nutzer ausgegebene Zeichenkette mit dem in dem Server-Rechnersystem (SF) abgelegten privaten Schlüssel (privK) verknüpft und mit der von dem Nutzer in die Client-Rechner-Arbeitsstation eingegebenen Antwortzeichenkette verglichen wird, und bei Übereinstimmung an die Client-Rechner-Arbeitsstation (CWS) eine erfolgreiche Authentifizierung signalisiert wird.

10. Verfahren zum Durchführen von kryptografischen Operationen in einem Server-Client-Rechnernetzwerksystem über ein Netzwerk (NW) zwischen einer Client-Rechner-Arbeitsstation (CWS) und einem Kryptografie-Server-Rechnersystem (KS), wobei
in der Client-Rechner-Arbeitsstation (CWS) und in dem Kryptografie-Server-Rechnersystem (KS) zur Kommunikation miteinander eingerichtete Computersoftware-Programme installiert sind und ausgeführt werden, damit, wenn die Client-Rechner-Arbeitsstation (CWS) eine Anfrage zum Durchführen einer kryptografischen Operation an das Kryptografie-Server-Rechnersystem (KS), diese von dem Kryptografie-Server-Rechnersystem (KS) beantwortet wird,
dadurch gekennzeichnet, dass
die Anfrage beantwortet wird, indem das Kryptografie-Server-Rechnersystem (KS) von der anfragenden Client-Rechner-Arbeitsstation (CWS) eine starke Authentifizierung anfordert,
worauf die Client-Rechner-Arbeitsstation (CWS) bei erfolgreicher Authentifizierung auf einen privaten Schlüssel (privK) ihres Nutzers zugreift, und
die Client-Rechner-Arbeitsstation (CWS) bei erfolgreicher Authentifizierung eine Freigabe dafür erhält, lediglich eine einzige oder wenige kryptografische Operationen mit dem privaten Schlüssel (privK) zu initiieren, wobei

- der private Schlüssel (privK) auf dem Kryptografie-Server-Rechnersystem (KS) abgelegt ist und nicht über das Netzwerk (NW) übertragen wird, sondern stets in dem Kryptografie-Server-Rechnersystem (KS) verbleibt, und
- die kryptografische/n Operation/en nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen wird/werden, um

die von einer auf der Client-Rechner-Arbeitsstation (CWS) ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en auszuführen, wobei
die Client-Rechner-Arbeitsstation (CWS) das Ergebnis der kryptografischen Operation/en der Applikationsprogramm-Software zur Verfügung stellt.

11. Verfahren nach Anspruch 10, bei dem die kryptografischen Operationen das Signieren eines Hashwertes oder das Entschlüsseln eines geheimen Schlüssels umfassen.

12. Verfahren nach Anspruch 10 oder11 bei dem das Kryptografie-Server-Rechnersystem (KS) zusätzlich einen Proxy Server (ProxS) und einen Authentifizierungs-Server (AuthS) hat.

13. Verfahren nach einem der Ansprüche 10 bis 12, bei dem
13.1. die starke Authentifizierung ein
13.1.1. für kurze Zeit gültiges, und/oder
13.1.2. einmaliges, und/oder
13.1.3. dynamisches
13.2. Legitimationsmittel ist, das zwischen der Client-Rechner-Arbeitsstation (CWS) und dem Kryptografie-Server-Rechnersystem (KS) ausgetauscht wird.

14. Verfahren nach Anspruch 13, bei dem das Legitimationsmittel ein Passwort oder ein Kennsatz ist.

15. Verfahren nach Anspruch 13 oder 14, bei dem die starke Authentifizierung in einem Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation (CWS) implementiert ist, wobei

15.1. das Computer-Softwareprogramm in der Client-Rechner-Arbeitsstation (CWS) einen Nutzer im Dialog auffordert, dessen ihn gegenüber dem Kryptografie-Server-Rechnersystem (KS) identifizierende Kennung einzugeben, und

15.2. nach Eingabe der Kennung des Nutzers die starke Authentifizierung anstößt.

16. Verfahren nach Anspruch 15, bei dem in dem Kryptografie-Server-Rechnersystem (KS)

16.1. die starke Authentifizierung überprüft wird, und

16.2. bei korrekter Authentifizierung an die Client-Rechner-Arbeitsstation (CWS) eine erfolgreiche Authentifizierung signalisiert wird.

17. Verfahren nach Anspruch 15, bei dem die Client-Rechner-Arbeitsstation (CWS) für den Nutzer nach Eingabe dessen Kennung eine Zeichenkette für den Nutzer ausgibt, die der Nutzer in eine separate Rechnereinheit einzugeben hat, die vorher mit einer gesicherten Chipkarte verbunden worden ist und mittels einer PIN frei geschaltet worden ist, worauf die separate Rechnereinheit mit der Chipkarte unter Anwendung einer Verknüpfungsvorschrift die Zeichenkette mit einem in der Chipkarte abgelegten Schlüssel verknüpft und dem Nutzer eine Antwortzeichenkette ausgibt, welche der Nutzer in die Client-Rechner-Arbeitsstation (CWS) einzugeben hat, und welche die Client-Rechner-Arbeitsstation (CWS) zur Authentifizierung an das Kryptografie-Server-Rechnersystem (KS) sendet.

18. Verfahren nach Anspruch 17, bei dem in dem Server-Rechnersystem (SF) unter Anwendung einer entsprechenden Verknüpfungsvorschrift die dem Nutzer ausgegebene Zeichenkette mit dem in dem Server-Rechnersystem (SF) abgelegten privaten Schlüssel (privK) verknüpft und mit der von dem Nutzer in die Client-Rechner-Arbeitsstation eingegebenen Antwortzeichenkette verglichen wird, und bei Übereinstimmung an die Client-Rechner-Arbeitsstation (CWS) eine erfolgreiche Authentifizierung signalisiert wird.

19. Server-Rechnersystem (SF), konfiguriert und programmiert zur Ausführung des vorstehend definierten Verfahrens.

20. Client-Rechner-Arbeitsstation (CWS), konfiguriert und programmiert zur Ausführung des vorstehend definierten Verfahrens.

21. Computerprogrammprodukt mit computerausführbaren Programm-Objektcode entsprechend dem vorstehend definierten Verfahren, der, wenn er in einem oder mehreren Computern ausgeführt wird, dazu eingerichtet ist, in einem Server-Client-Rechnernetzwerksystem eine sichere Rechnernetzwerkverbindung nach einem der vorhergehenden Ansprüche zu bewirken.

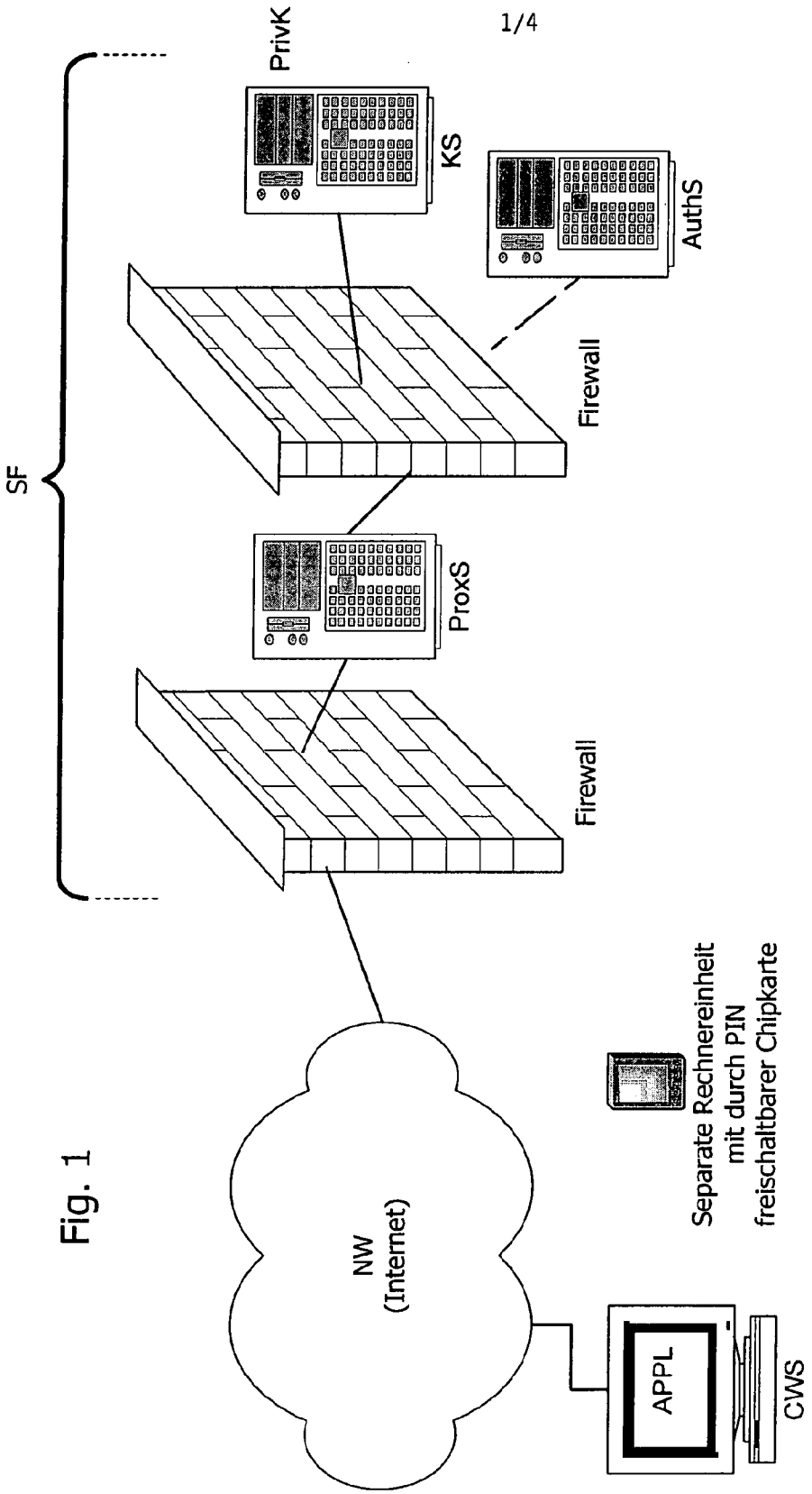

SF
PrivK
KS
AuthS
Firewall
ProxS
Firewall
NW
(Internet)
Separate Rechnereinheit
mit durch PIN
freischaltbarer Chipkarte
APPL
CWS

Fig. 1

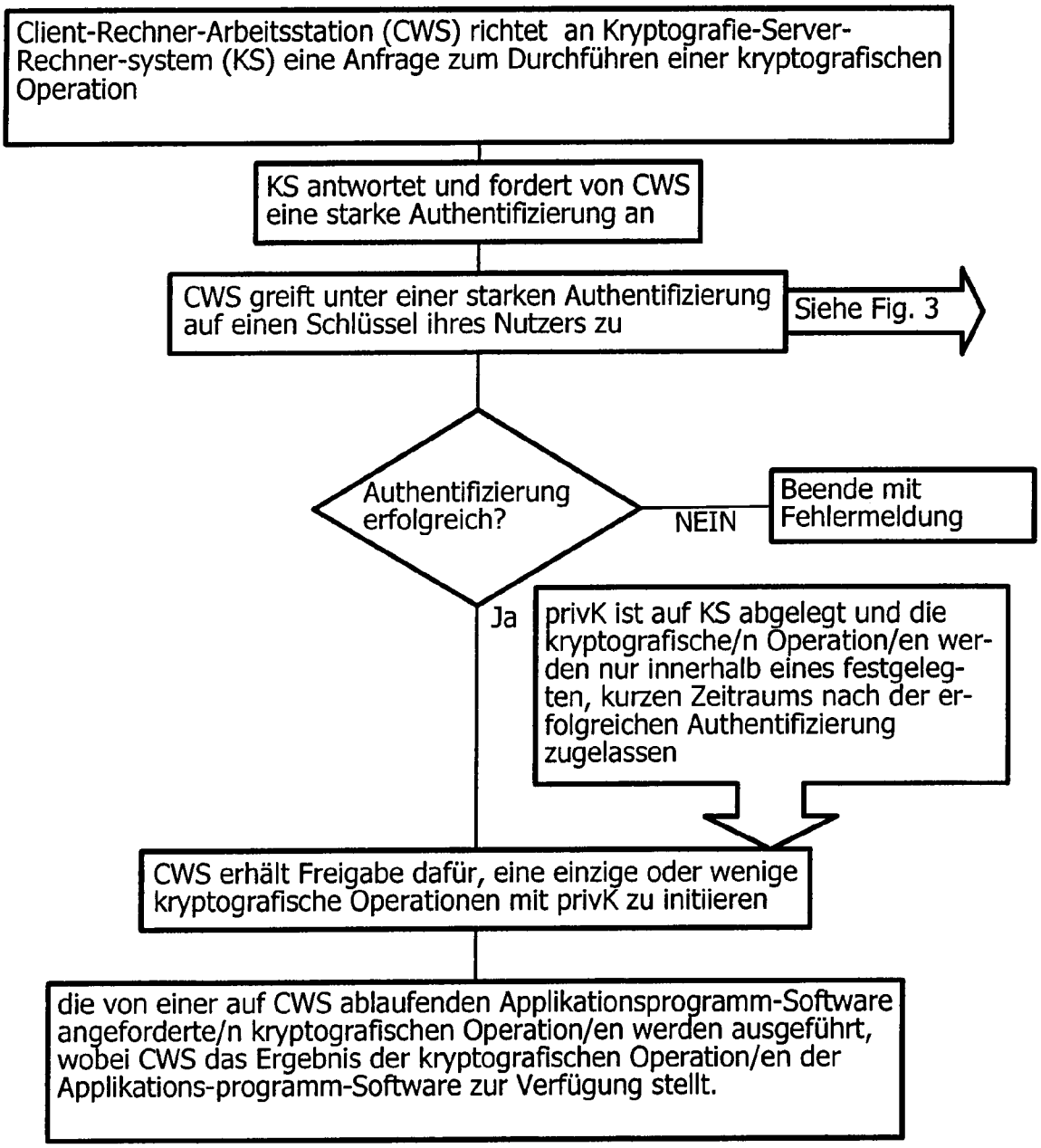

Client-Rechner-Arbeitsstation (CWS) richtet an Kryptografie-Server-Rechner-system (KS) eine Anfrage zum Durchführen einer kryptografischen Operation
KS antwortet und fordert von CWS eine starke Authentifizierung an
CWS greift unter einer starken Authentifizierung auf einen Schlüssel ihres Nutzers zu
Siehe Fig. 3
Authentifizierung erfolgreich?
NEIN
Beende mit Fehlermeldung
Ja
privK ist auf KS abgelegt und die kryptografische/n Operation/en werden nur innerhalb eines festgelegten, kurzen Zeitraums nach der erfolgreichen Authentifizierung zugelassen
CWS erhält Freigabe dafür, eine einzige oder wenige kryptografische Operationen mit privK zu initiieren
die von einer auf CWS ablaufenden Applikationsprogramm-Software angeforderte/n kryptografischen Operation/en werden ausgeführt, wobei CWS das Ergebnis der kryptografischen Operation/en der Applikations-programm-Software zur Verfügung stellt.

Fig. 2

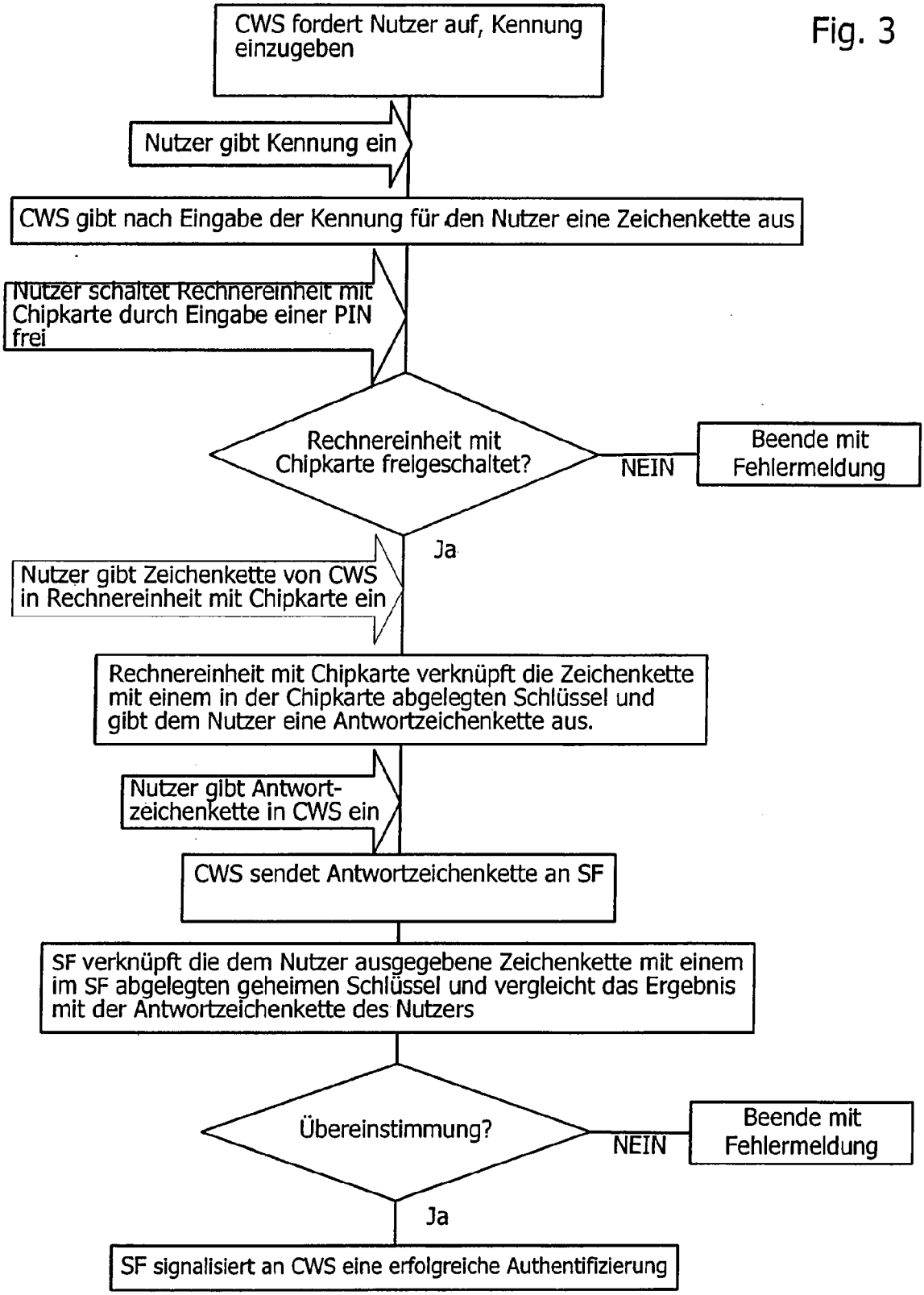
Fig. 2a

kryptografische Operationen	
Signieren eines Hashwertes	Entschlüsseln eines Schlüssels
	geheimer Schlüssel
	privater Schlüssel
	a/symmetrischer Schlüssel

Für die starke Authentifizierung verwendete Legitimationsmittel sind
* alpha/numerische Zeichenketten (4 ... 20 Stellen)
* für kurze Zeit gültig (0,2 ... 5 min)
* nur einmal gültig
* dynamisch erzeugt

Fig. 2b

Fig. 3


CWS fordert Nutzer auf, Kennung einzugeben
Nutzer gibt Kennung ein
CWS gibt nach Eingabe der Kennung für den Nutzer eine Zeichenkette aus
Nutzer schaltet Rechnereinheit mit Chipkarte durch Eingabe einer PIN frei
Rechnereinheit mit Chipkarte freigeschaltet?
NEIN
Beende mit Fehlermeldung
Ja
Nutzer gibt Zeichenkette von CWS in Rechnereinheit mit Chipkarte ein
Rechnereinheit mit Chipkarte verknüpft die Zeichenkette mit einem in der Chipkarte abgelegten Schlüssel und gibt dem Nutzer eine Antwortzeichenkette aus.
Nutzer gibt Antwort-zeichenkette in CWS ein
CWS sendet Antwortzeichenkette an SF
SF verknüpft die dem Nutzer ausgegebene Zeichenkette mit einem im SF abgelegten geheimen Schlüssel und vergleicht das Ergebnis mit der Antwortzeichenkette des Nutzers
Übereinstimmung?
NEIN
Beende mit Fehlermeldung
Ja
SF signalisiert an CWS eine erfolgreiche Authentifizierung

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/009861

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2001/014158 A1 (BALTZLEY CLIFF A) 16 August 2001 (2001-08-16) paragraphs [0010], [0011]	1-21
Y	WO 01/48948 A (TELEFONAKTIEBOLAGET LM ERICSSON ; BALACHANDRAN, SHRIDHARAN; ALPEROVICH) 5 July 2001 (2001-07-05) page 3, line 14 - page 4, line 13; claim 25	1-21

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2006	20/12/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/009861

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001014158 A1	16-08-2001	NONE	
WO 0148948 A	05-07-2001	AT 326798 T	15-06-2006
		AU 3266001 A	09-07-2001
		EP 1243088 A1	25-09-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2006/009861

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2001/014158 A1 (BALTZLEY CLIFF A) 16. August 2001 (2001-08-16) Absätze [0010], [0011]	1-21
Y	WO 01/48948 A (TELEFONAKTIEBOLAGET LM ERICSSON ; BALACHANDRAN, SHRIDHARAN; ALPEROVICH) 5. Juli 2001 (2001-07-05) Seite 3, Zeile 14 - Seite 4, Zeile 13; Anspruch 25	1-21

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
11. Dezember 2006	20/12/2006

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Veen, Gerardus

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2006/009861

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2001014158 A1	16-08-2001	KEINE	
WO 0148948 A	05-07-2001	AT 326798 T	15-06-2006
		AU 3266001 A	09-07-2001
		EP 1243088 A1	25-09-2002